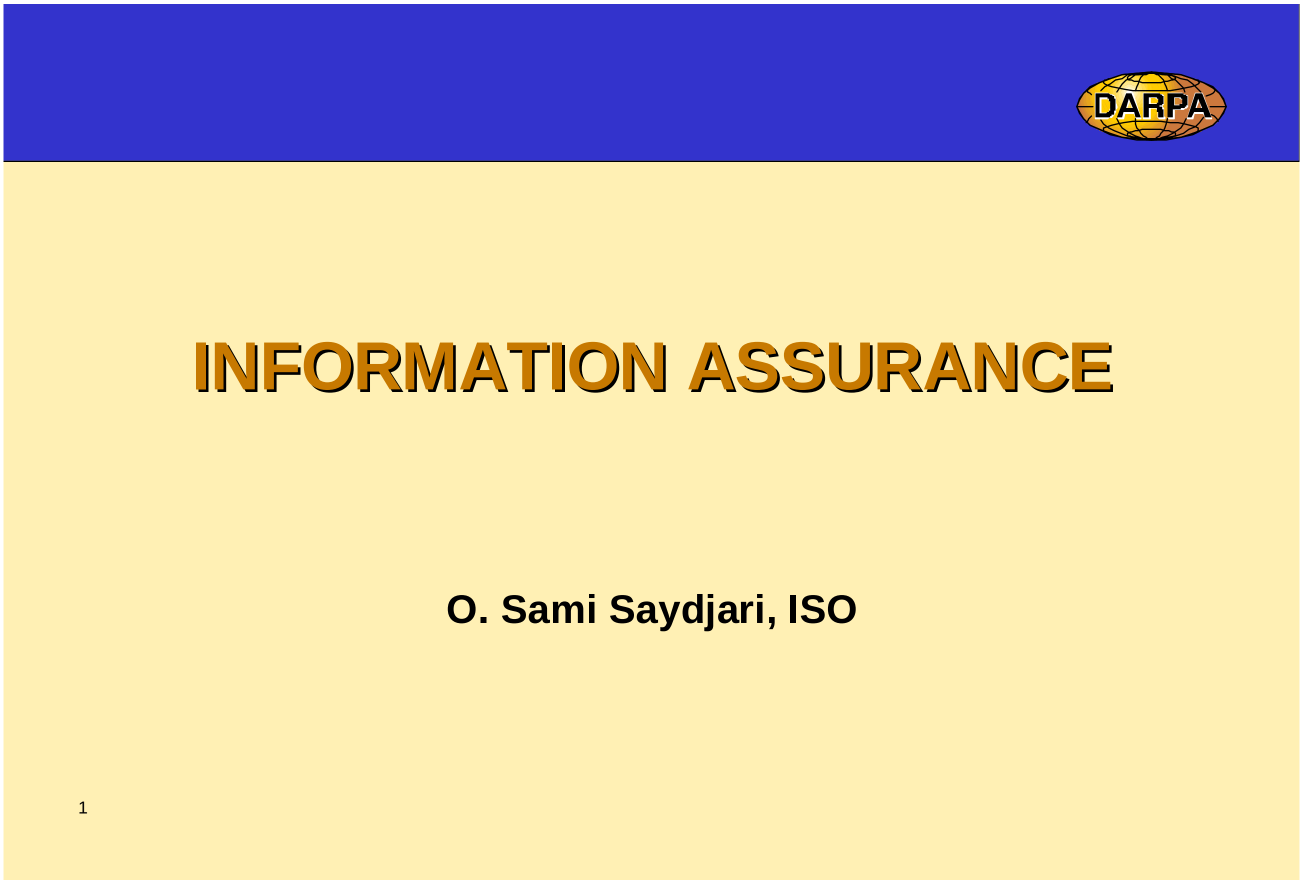
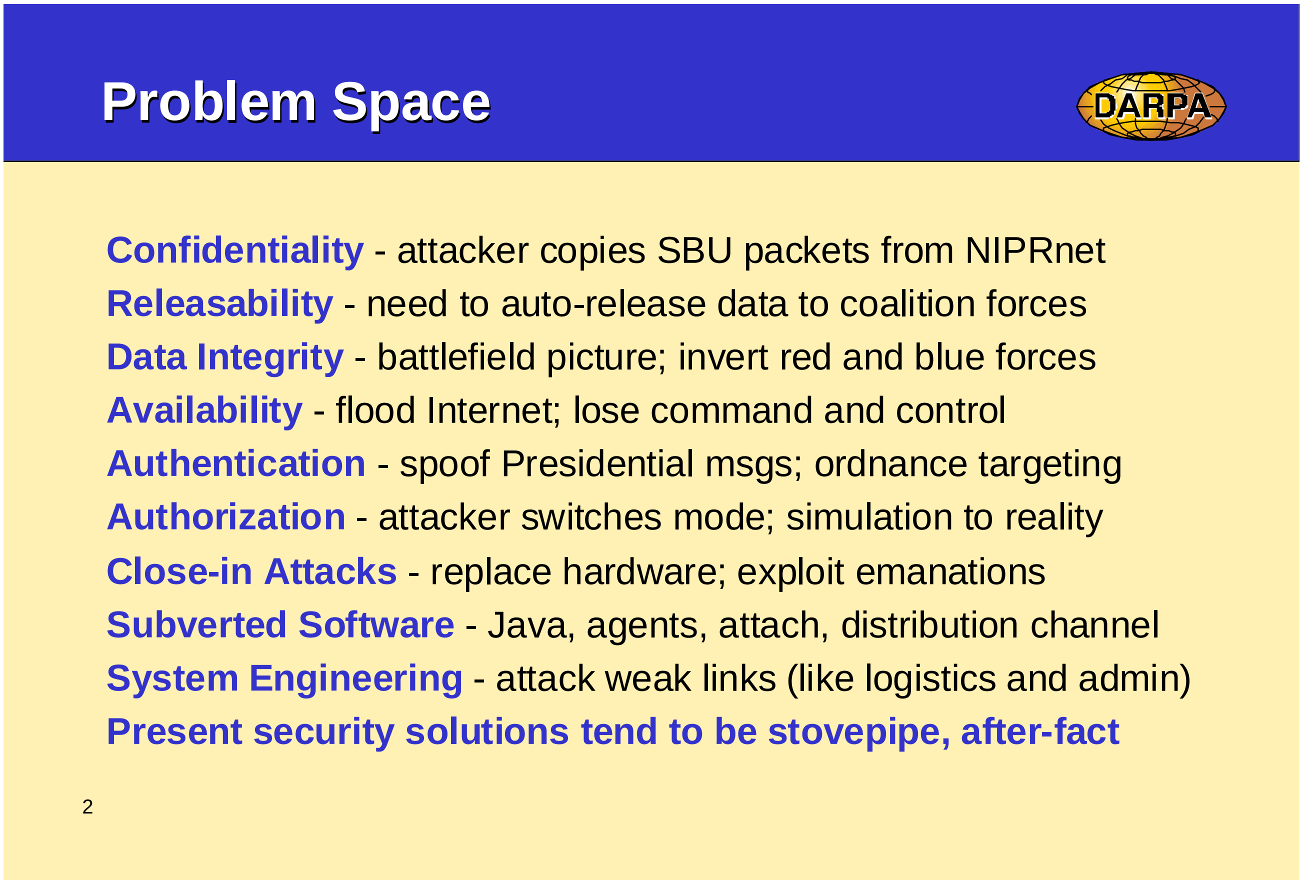


INFORMATION ASSURANCE

O. Sami Saydjari, ISO

1



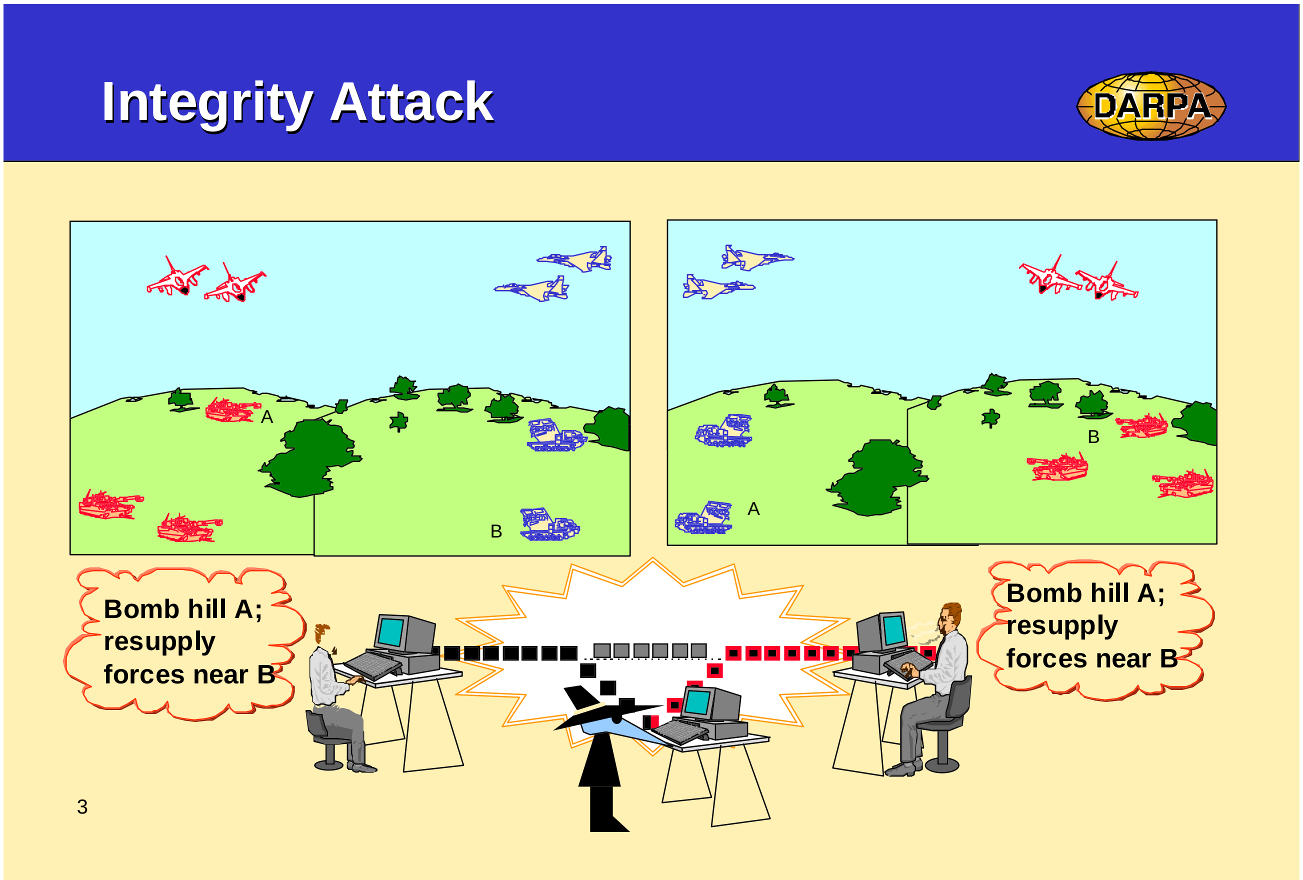
Problem Space

DARPA

Confidentiality - attacker copies SBU packets from NIPRnet
Releasability - need to auto-release data to coalition forces
Data Integrity - battlefield picture; invert red and blue forces
Availability - flood Internet; lose command and control
Authentication - spoof Presidential msgs; ordnance targeting
Authorization - attacker switches mode; simulation to reality
Close-in Attacks - replace hardware; exploit emanations
Subverted Software - Java, agents, attach, distribution channel
System Engineering - attack weak links (like logistics and admin)
Present security solutions tend to be stovepipe, after-fact

This slide outlines the many security problems facing the military community.

- Confidentiality - an adversary copies information from your system without your knowledge.
- Releasability is a major issue in provision of data to allies - automation of release functions will expedite information exchange significantly.
- Data Integrity will be a major problem in the battlefield, particularly in the face of an Info Warfare savvy enemy. It is possible to inject modifications in data streams such that a receiving commander makes erroneous decisions.
- Availability - flooding the Internet such that it is unusable is a real and present threat. Tools are available to hackers on the Internet now that could blind a commander.
- Authentication continues to be a major concern - did that message really come from the Task Force Commander or from the enemy?
- Authorization is another major problem - for example, an enemy could switch C3 circuit mode from operational to simulation and provide commanders bogus information.
- Close-in Attacks - adversary gains access to hardware and modifies.
- Subverted Software agents on the Internet are a significant threat.
- System Engineering attacks, e.g., logistics systems, could be fatal.

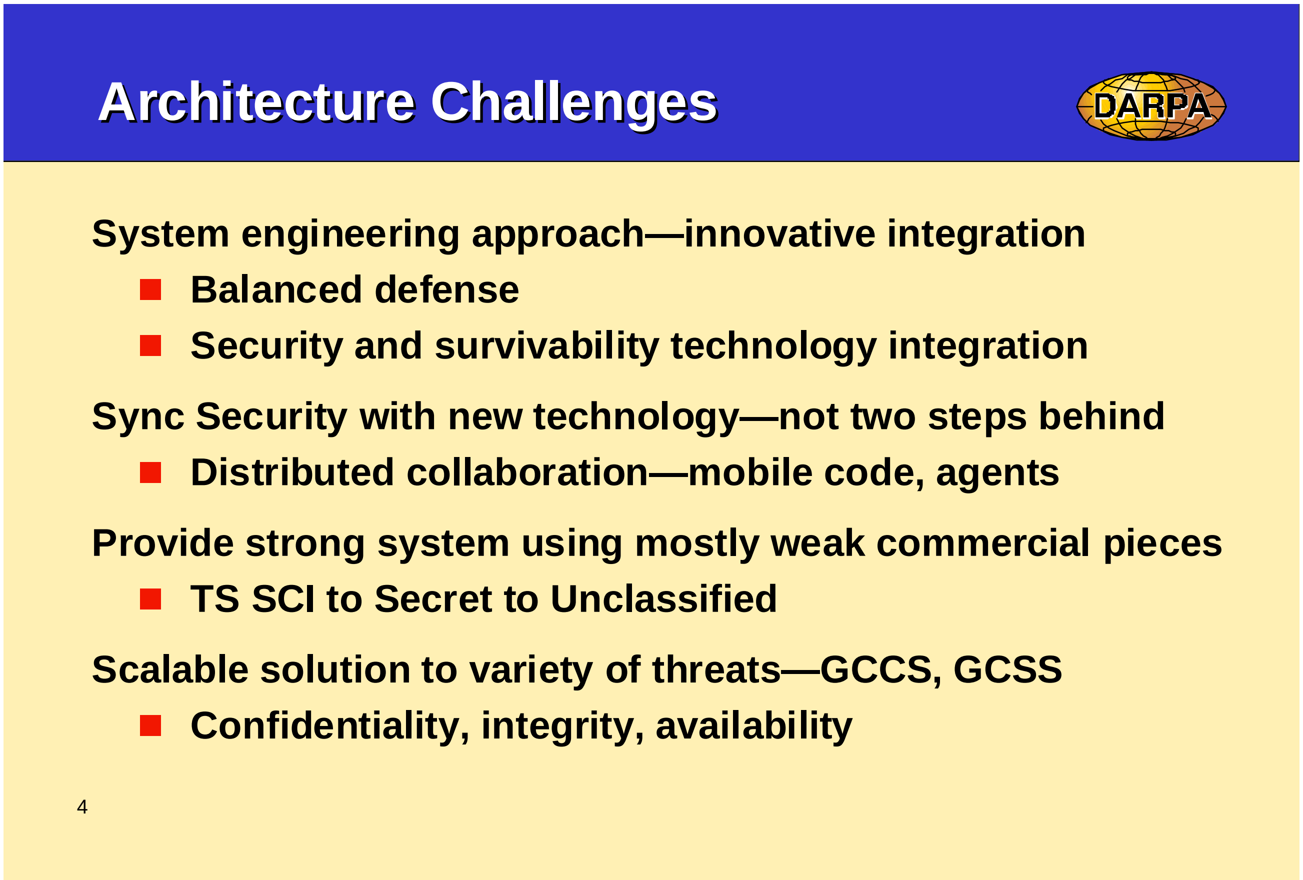


Integrity Attack

DARPA
A
B
B
A
Bomb hill A; resupply forces near B
Bomb hill A; resupply forces near B

3

In this example, the good guy on the left sends a picture of the battlefield to a good-guy colleague on the right. Unbeknownst to either, the bad-guy in the middle intercepts the picture and changes it, causing the person on the right to issue damaging orders.



Architecture Challenges

System engineering approach—innovative integration

- Balanced defense
- Security and survivability technology integration

Sync Security with new technology—not two steps behind

- Distributed collaboration—mobile code, agents

Provide strong system using mostly weak commercial pieces

- TS SCI to Secret to Unclassified

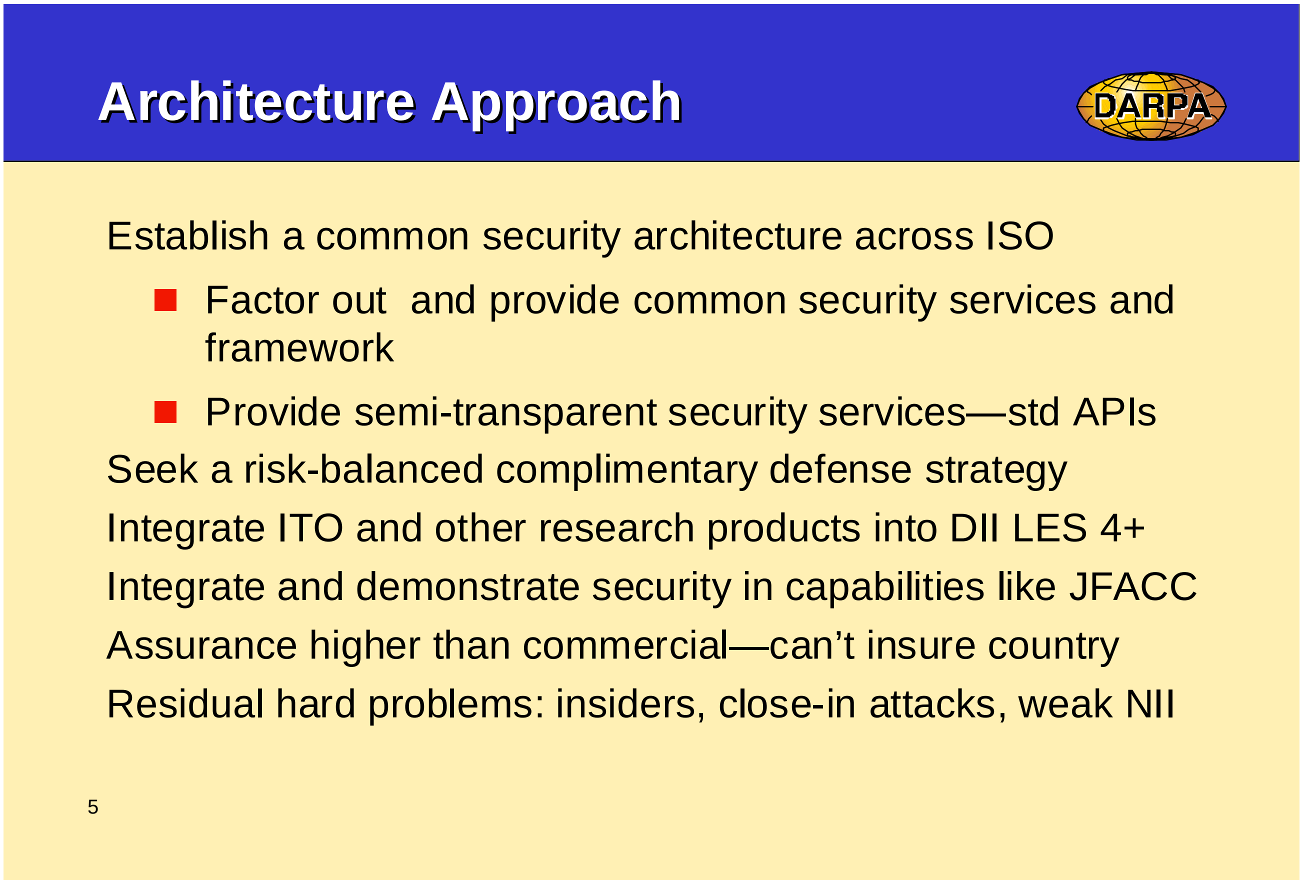
Scalable solution to variety of threats—GCCS, GCSS

- Confidentiality, integrity, availability

The primary architecture challenge is integration of security technology to provide a balanced defense which allows collaboration across the full range of classification levels.

We need to put security in synch with developing systems and not lag the problem as is frequently the case - security is often an after thought as the system is being developed.

We seek to build a strong system using mostly commercial off-the-shelf technologies. These technologies must be cleverly integrated to allow scalability while maintaining requisite security.



Architecture Approach

Establish a common security architecture across ISO

- Factor out and provide common security services and framework
- Provide semi-transparent security services—std APIs

Seek a risk-balanced complimentary defense strategy

Integrate ITO and other research products into DII LES 4+

Integrate and demonstrate security in capabilities like JFACC

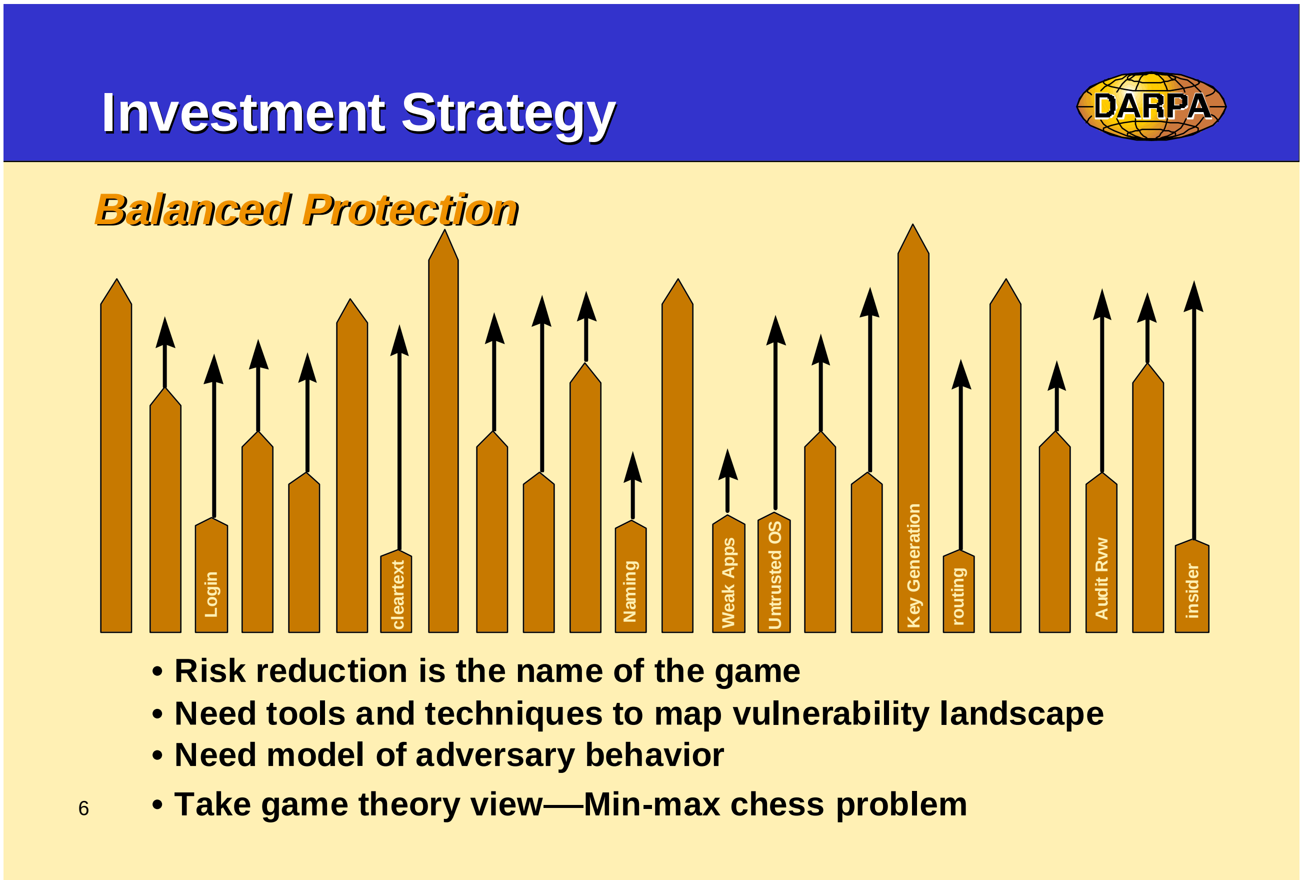
Assurance higher than commercial—can't insure country

Residual hard problems: insiders, close-in attacks, weak NII

5

The Information Assurance Program strategy is based on a systems level view of assurance problems and taking a systems engineering approach. Key is a balanced approach that seeks to integrate security and survivability technology in mutually complementary ways. We want to use tools available in the commercial world to best advantage - integrated smartly - rather than develop grand new applications. Major tenants of the DARPA approach:

- We need to synchronize security with new information technology as the technology becomes available rather than waiting until the technology is field ready and then worrying about securing it.
- Establish common security services and Information Assurance framework for use throughout DOD.
- Lead commercial security - DOD security is a harder requirement that you can't take out an insurance policy from Lloyds to cover.
- Key goal is that security services be semi-transparent through standard API. Users should not have to devote time, energy, and frustration to satisfy security "wickets."
- Information Assurance services and tools will be integrated into and demonstrated with information programs such as JFACC and BADD rather than being developed and demonstrated in isolation.
- ITO technologies and other new development products will be integrated into GCCS LES through the ISO integrated testbed architecture and JPO Virtual Collaboratory.



Investment Strategy

DARPA

Balanced Protection

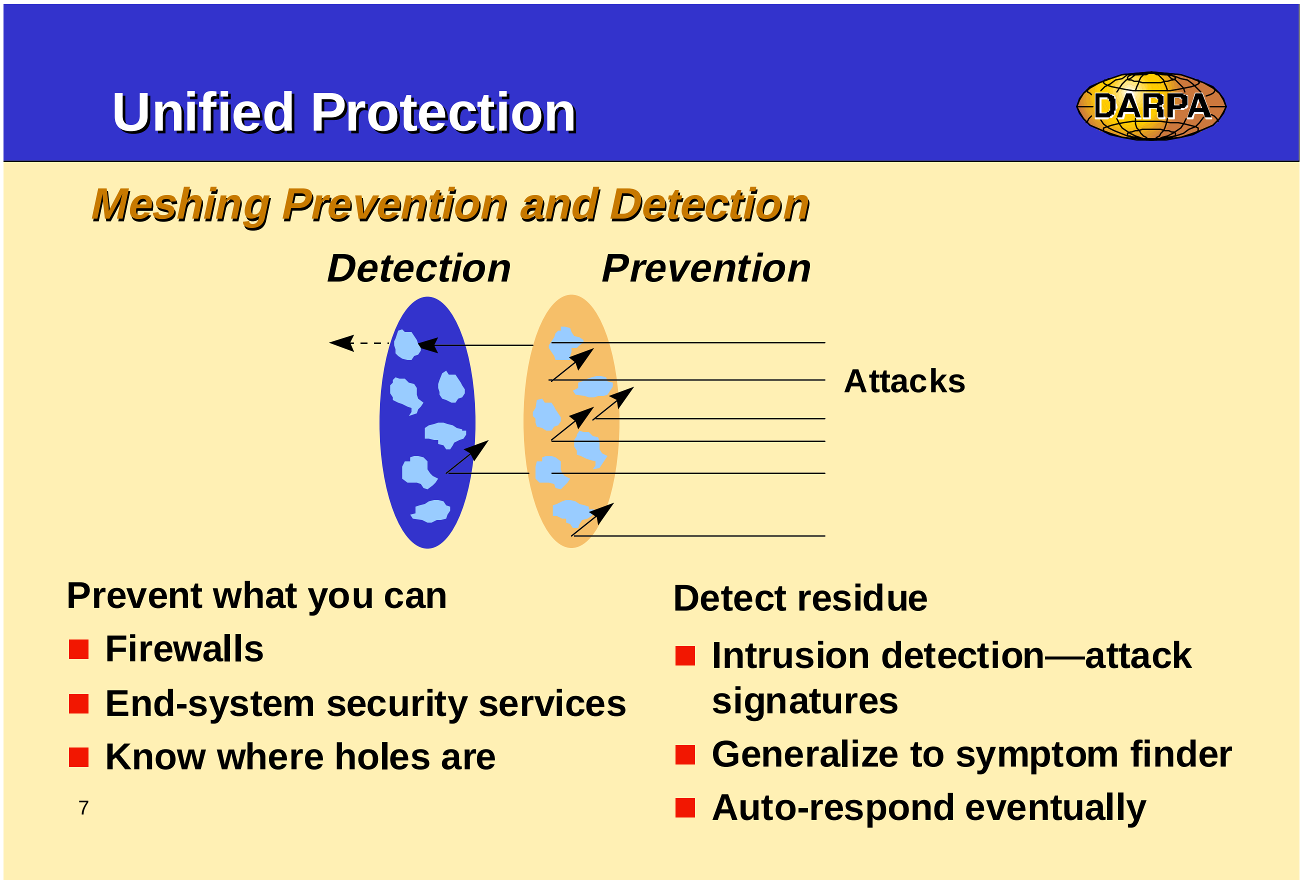
- **Risk reduction is the name of the game**
- **Need tools and techniques to map vulnerability landscape**
- **Need model of adversary behavior**
- **Take game theory view—Min-max chess problem**

6

This slide endeavors to show an “information defense fence.” The “pickets” or components of the fence provide varying degrees of protection. An adversary will seek to exploit the “low pickets” or weak components of the fence. For example, it makes little sense to have an elegant crypto system riding on an untrusted operating system.

Risk assessment and reduction are essential to the success of the program. We must balance the risks to reach achievable, cost-effective information assurance.

Tools to assess risk are needed as well as effective adversary behavior models.



Unified Protection

Meshing Prevention and Detection

Prevent what you can

- **Firewalls**
- **End-system security services**
- **Know where holes are**

Detect residue

- **Intrusion detection—attack signatures**
- **Generalize to symptom finder**
- **Auto-respond eventually**

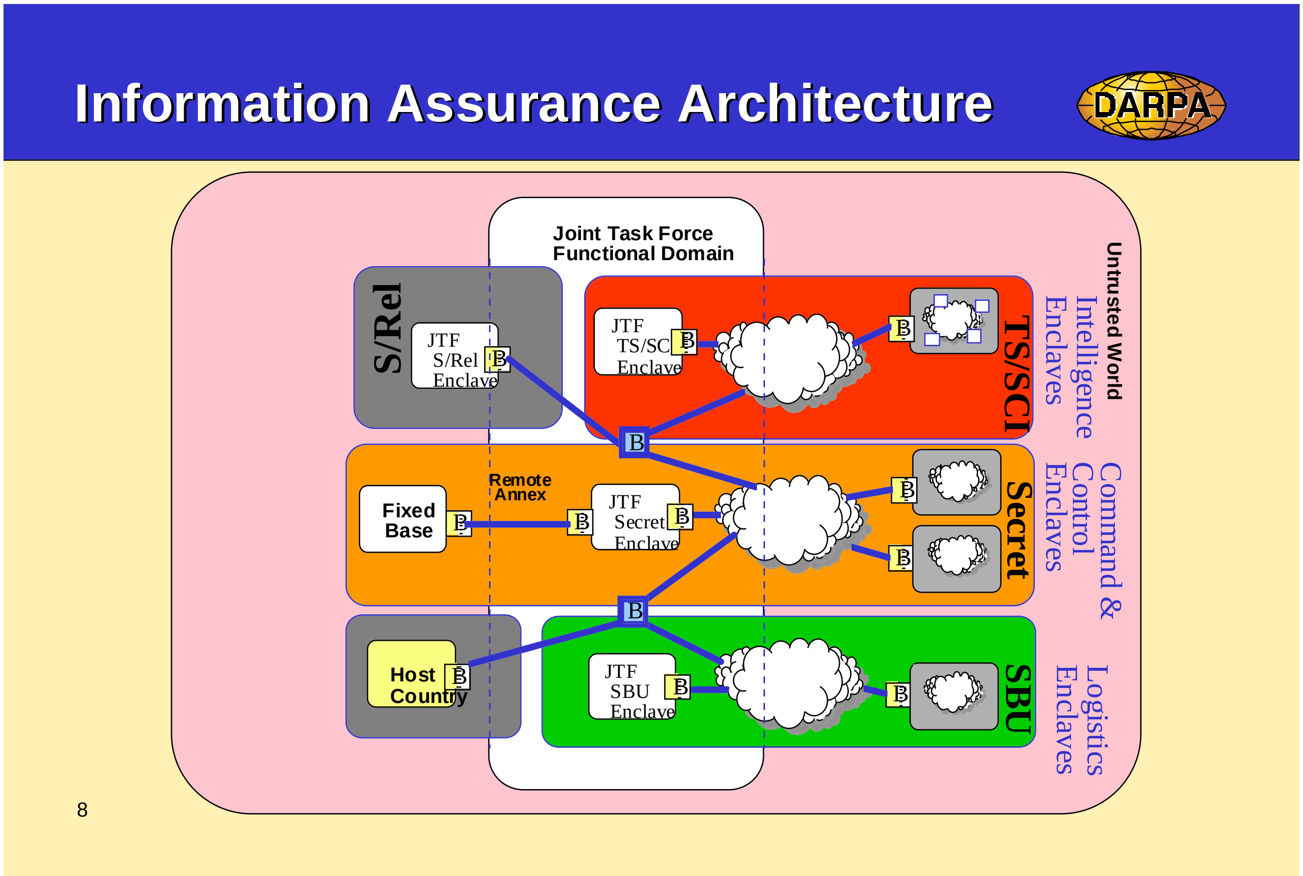
7

Here we pictorially show the layers of defense envisioned with protection disks. The disks have holes where an attacker may gain access to an enclave. It is impossible to achieve 100% assurance - so we seek to achieve acceptable levels of protection by aligning the disks so that minimal attacks get through.

We establish prevention layers at the boundaries of information enclaves as a first line of defense. Firewalls, guards, boundary controllers, for example, form the prevention layer.

Attacks that pass through the prevention layer are detected by auto-detection tools, and the attack is thwarted by isolating the attack. Eventually, system auto-reconfiguration will automatically isolate an attacker.

Some attack may pass through both disks - robust back-up and recovery systems are needed here.



Information Assurance Architecture

8

This slide depicts the security architecture and the use of protected enclaves:

Limited multilevel security capabilities

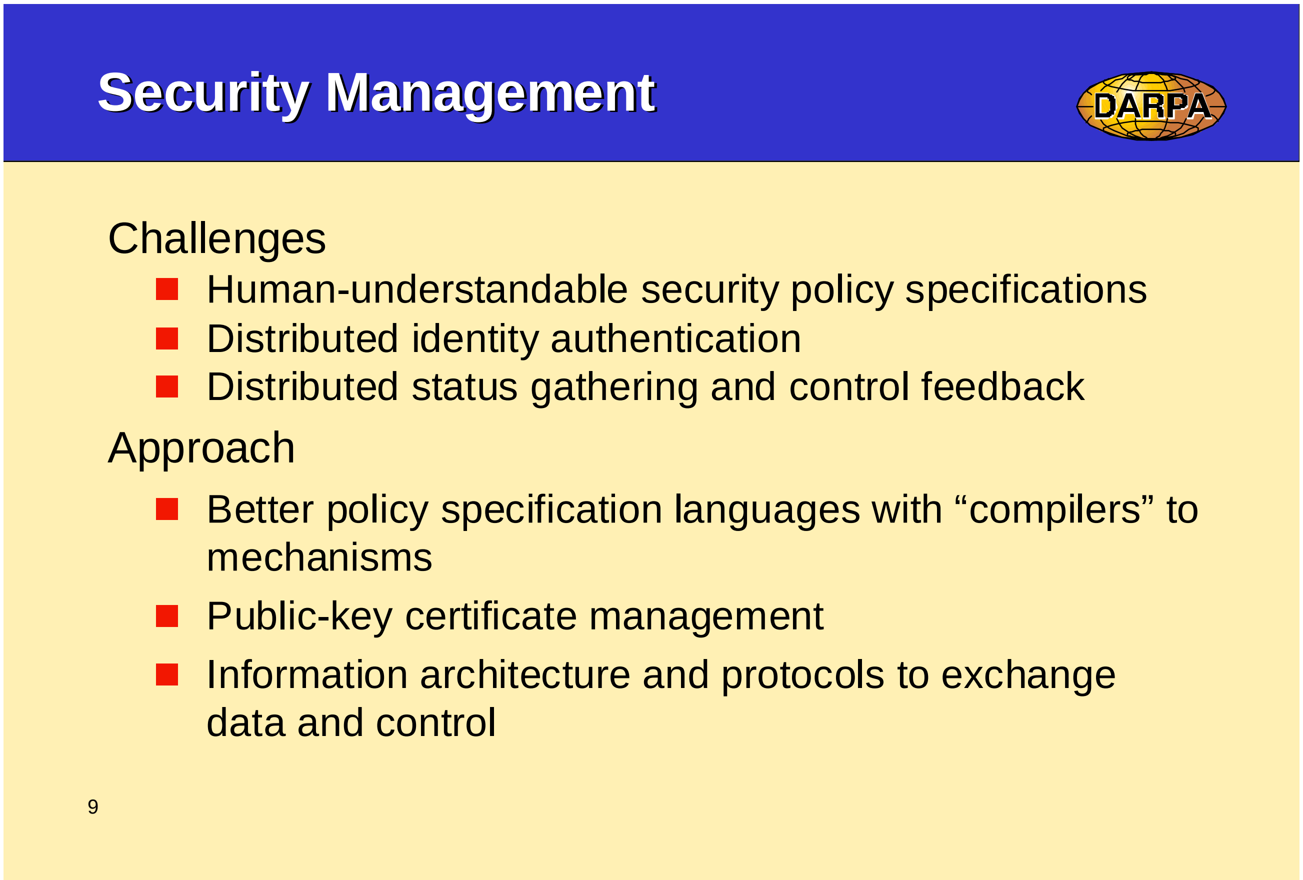
- System high enclaves with boundary controllers
  - Guards across security level and coalition domains
  - Firewalls within security level and coalition domains
- Data labeling at source for automated release by guards

Scalable, layered cryptographic support

- Certificates and public key infrastructure for authentication, attribute-based access control, ...
- Strong encryption between enclaves, weaker (cheaper) encryption within enclaves

Use CORBA Security plus other COTS interfaces and tools (e.g., for authorization management)

Addition of security-specific AITS RA servers and applications



Security Management

Challenges

- Human-understandable security policy specifications
- Distributed identity authentication
- Distributed status gathering and control feedback

Approach

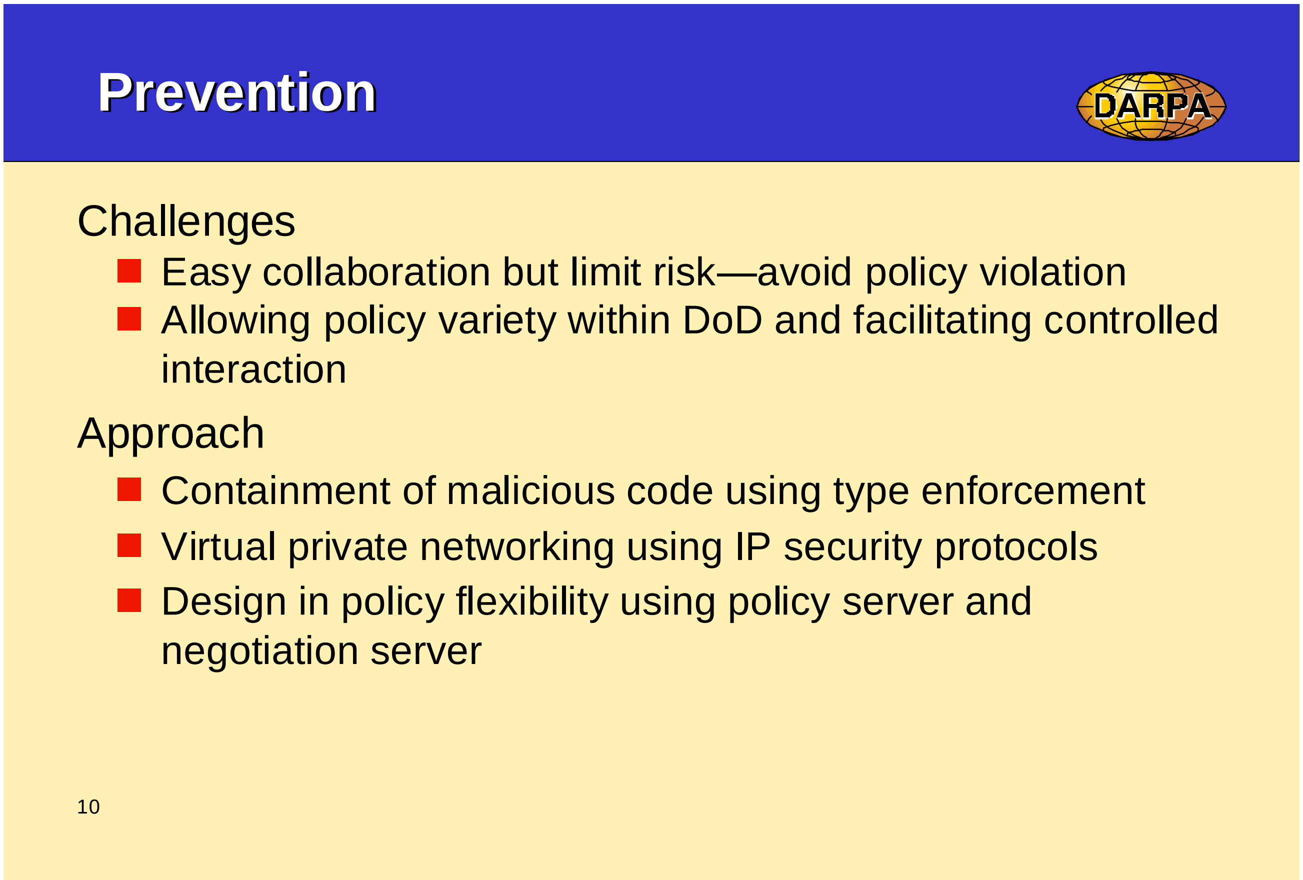
- Better policy specification languages with “compilers” to mechanisms
- Public-key certificate management
- Information architecture and protocols to exchange data and control

9

Manage System Security

A security management infrastructure is being developed to support policy specification and security services such as global identification of users, and exchange and certification of cryptographic keys. The components of this infrastructure and the traffic among them will be protected.

A security anchor desk that maintains watch over system state and defensive posture is a key element of system management.



Prevention

Challenges

- Easy collaboration but limit risk—avoid policy violation
- Allowing policy variety within DoD and facilitating controlled interaction

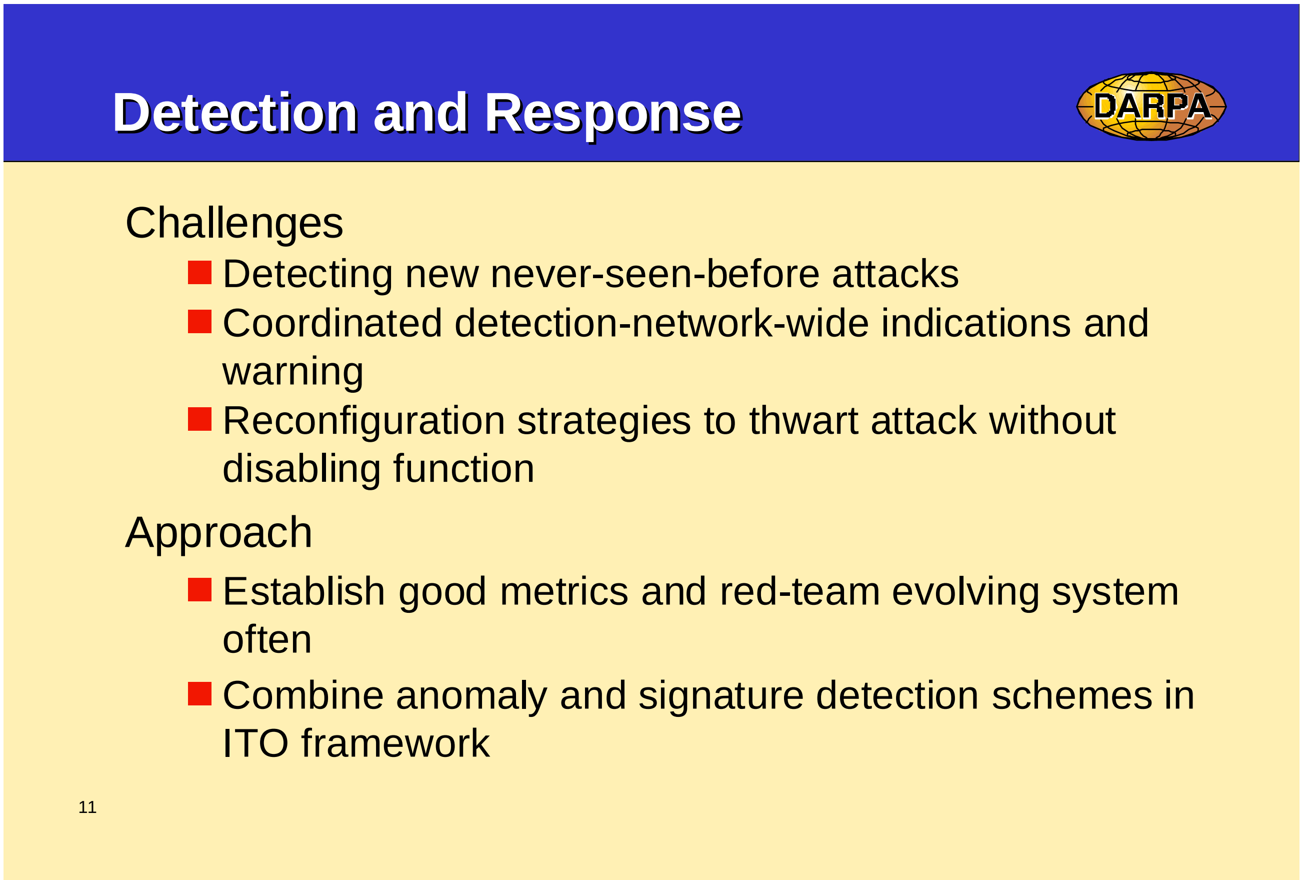
Approach

- Containment of malicious code using type enforcement
- Virtual private networking using IP security protocols
- Design in policy flexibility using policy server and negotiation server

10

Prevent Attack Opportunity - Control Access

Data that is integral to current and planned ISO-developed systems and that is openly stored and transmitted on public networks is available to any adversary and can allow inference of more highly sensitive information. Solutions to be integrated include encryption of message traffic, firewalls, and program and data authentication (e.g., within end systems and network routers).



Detection and Response

Challenges

- Detecting new never-seen-before attacks
- Coordinated detection-network-wide indications and warning
- Reconfiguration strategies to thwart attack without disabling function

Approach

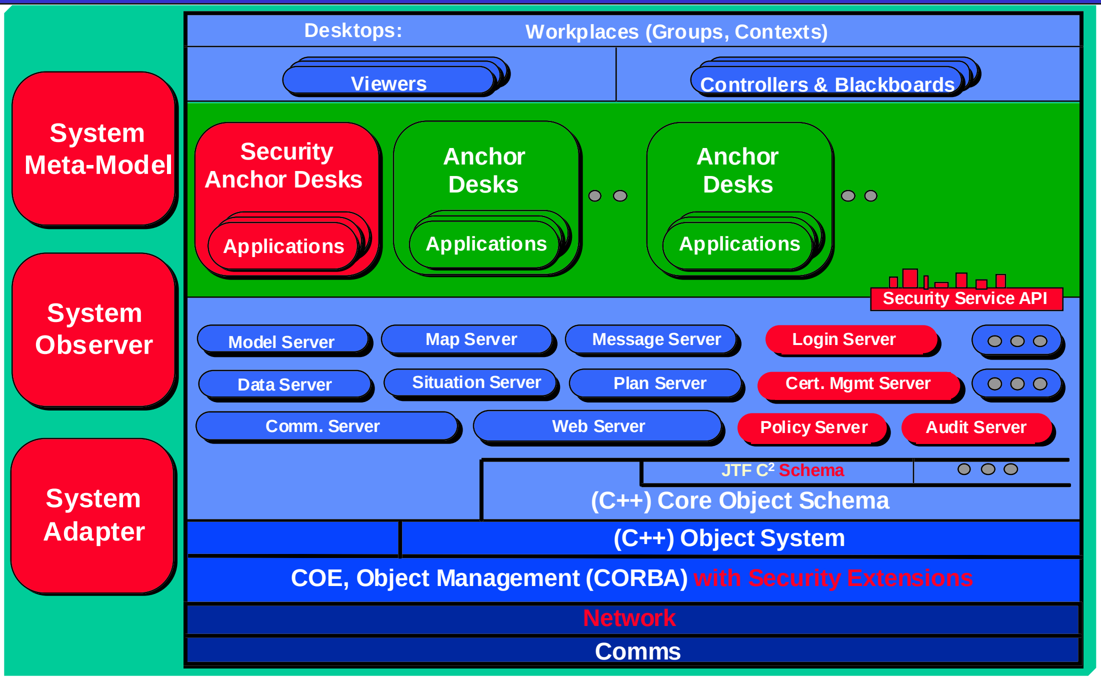
- Establish good metrics and red-team evolving system often
- Combine anomaly and signature detection schemes in ITO framework

Detect and Respond to Unprevented Attack

Because vulnerability cannot be eliminated, attack detection methods will be integrated. Through experimentation in real systems, we will reduce false alarm rates and enhance real-time detection capability. We will build in automated and context-sensitive response capability, such as adding filters to firewalls and routers, selectively shutting down resources, rerouting traffic, and running only authenticated software.

Extended Reference Architecture

DARPA



Desktops:

Workplaces (Groups, Contexts)

Viewers

Controllers & Blackboards

System Meta-Model

System Observer

System Adapter

Security Anchor Desks

Applications

Anchor Desks

Applications

Anchor Desks

Applications

Security Service API

Model Server

Map Server

Message Server

Login Server

Data Server

Situation Server

Plan Server

Cert. Mgmt Server

Comm. Server

Web Server

Policy Server

Audit Server

JTF C^2 Schema

(C++) Core Object Schema

(C++) Object System

COE, Object Management (CORBA) with Security Extensions

Network

Comms

12

Limited multilevel security capabilities

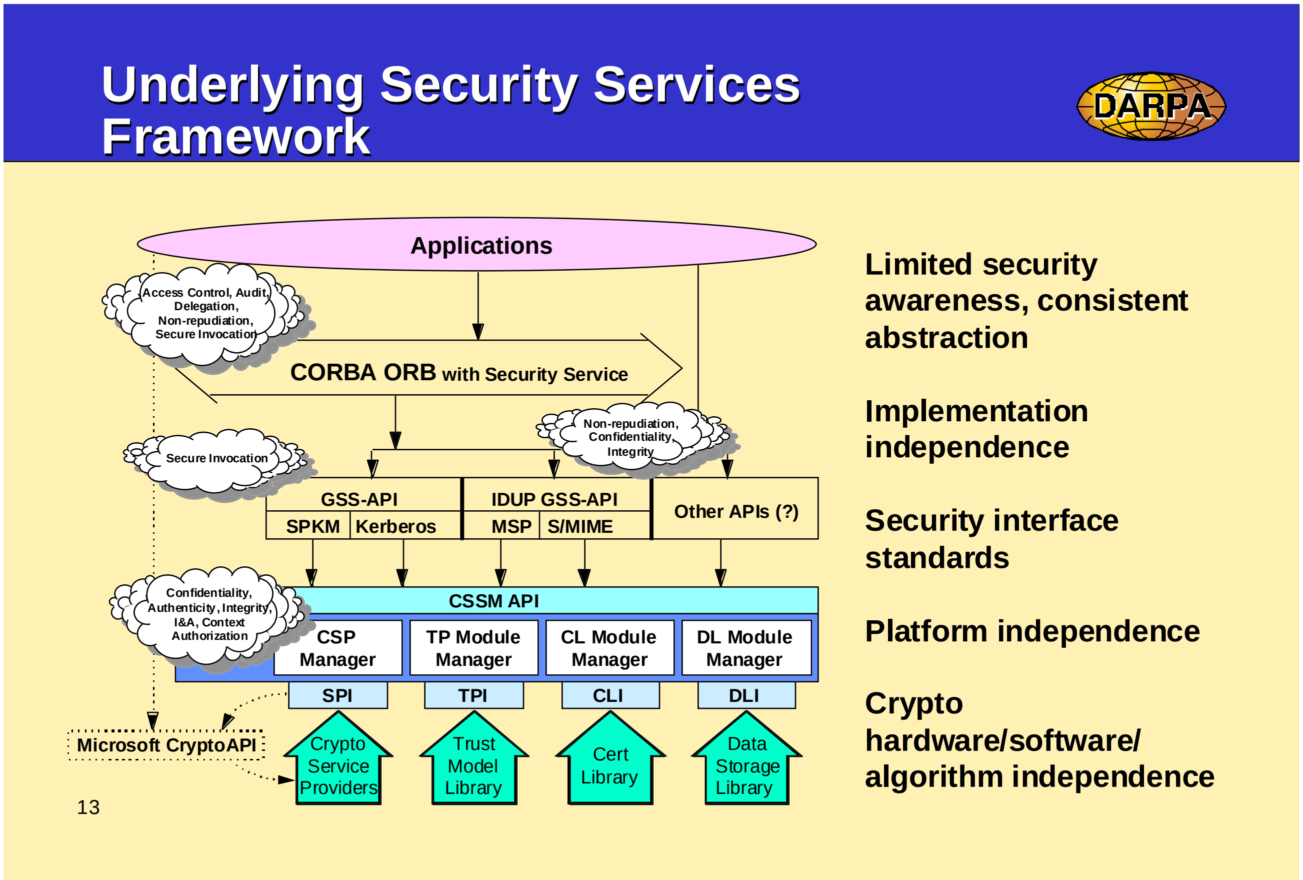
- System high enclaves with boundary controllers
  - Guards across security level and coalition domains
  - Firewalls within security level and coalition domains
- Data labeling at source for automated release by guards

Scalable, layered cryptographic support

- Certificates and public key infrastructure for authentication, attribute-based access control, ...
- Strong encryption between enclaves, weaker (cheaper) encryption within enclaves

Use of CORBA Security supplemented with other COTS interfaces and tools (e.g., for authorization management)

Addition of security-specific AITS RA servers and applications



Underlying Security Services Framework

Limited security awareness, consistent abstraction

Implementation independence

Security interface standards

Platform independence

Crypto hardware/software/ algorithm independence

The security API framework identifies the layering of security services and interfaces that underlie the security-extended AITS-RA. The floating clouds indicate the security services the API provides.

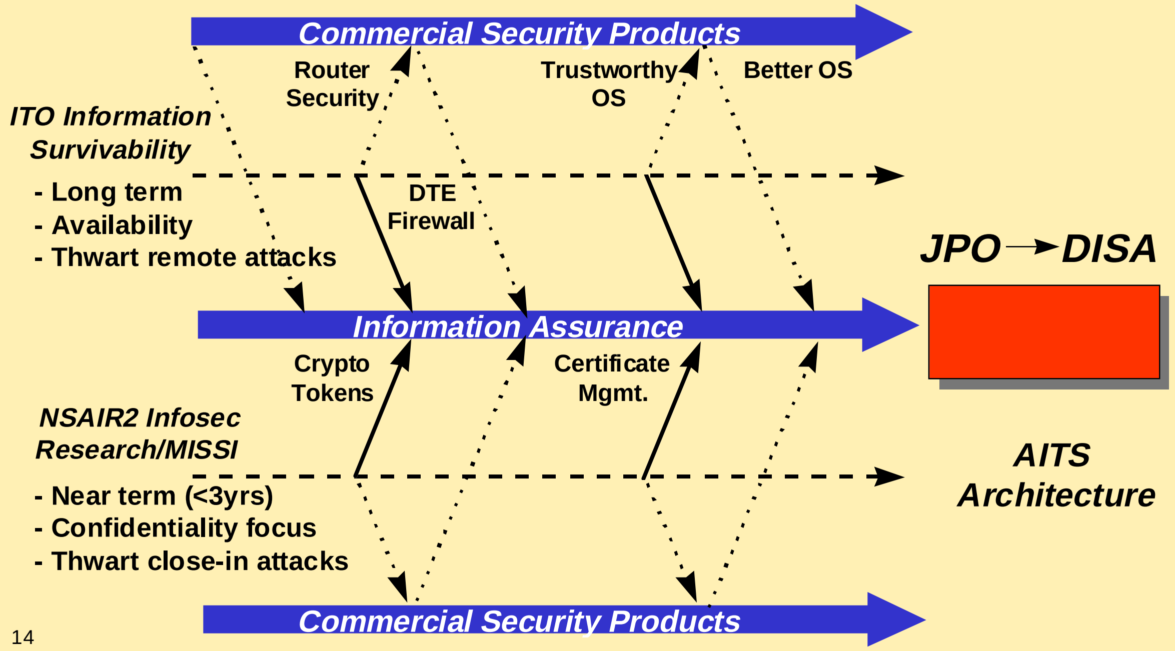
The security API framework base level is Intel’s CDSA. CDSA is intended to provide a cryptographic services middleware layer with a plug-in capability for hardware. The cryptographic and certificate layer used to construct higher level security services, such as distributed authentication or access control. This allows cryptographically based security services to be provided with a degree of platform and cryptographic algorithm-independence.

An additional layer above CDSA provides other security service APIs, such as Simple Public Key Mechanism (SPKM) and Kerberos.

Above this layer, security services defined in CORBASEC are provided.

The security API framework provides security services at the system infrastructure and middleware levels to provide a firm foundation for security functions that extend up through the server and application layers.

Security Technology Integration



Commercial Security Products

Router Security

Trustworthy OS

Better OS

ITO Information Survivability

- Long term
- Availability
- Thwart remote attacks

DTE Firewall

Information Assurance

Crypto Tokens

Certificate Mgmt.

NSAIR2 Infosec Research/MISSI

- Near term (<3yrs)
- Confidentiality focus
- Thwart close-in attacks

Commercial Security Products

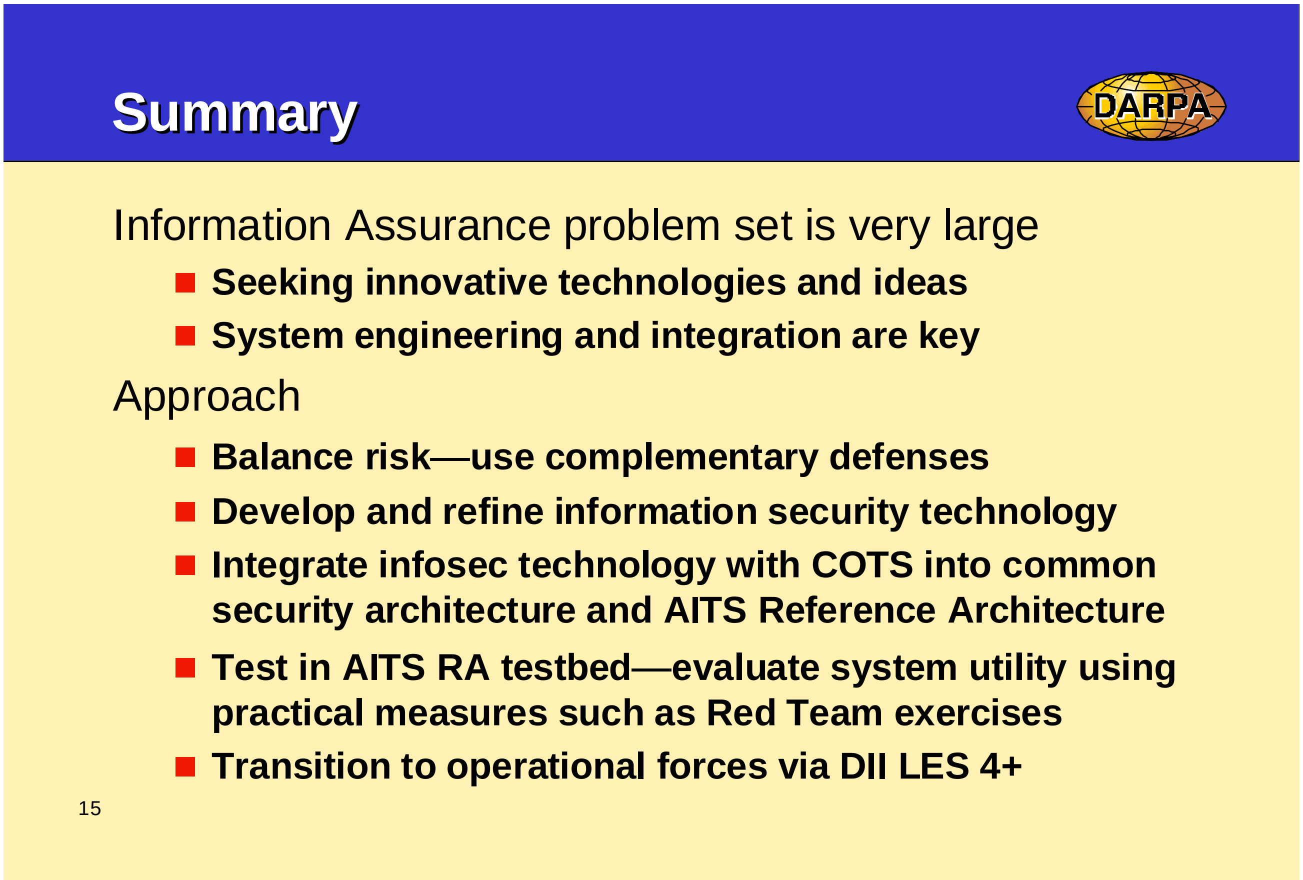
JPO → DISA

AITS Architecture

Fundamental to the success of the Information Assurance Program is coordination with other programs and agencies. Information Assurance should be systemic - imbedded in each program - to enable the program, such as JFACC or BADD, to function with a sense of information well-being.

The IA Program will be cooperating and coordinating with a number of programs and offices, such as ITO, JPO, NSA, and the military services to accomplish its mission.

Technologies developed by ITO and under the IA program will be integrated into the Security Architecture. These technologies and tools will be tested in the Integrated Testbed Collaboratory - Virtual Collaboratory - by the JPO for transition to the military services.



Summary

Information Assurance problem set is very large

- Seeking innovative technologies and ideas
- System engineering and integration are key

Approach

- Balance risk—use complementary defenses
- Develop and refine information security technology
- Integrate infosec technology with COTS into common security architecture and AITS Reference Architecture
- Test in AITS RA testbed—evaluate system utility using practical measures such as Red Team exercises
- Transition to operational forces via DII LES 4+

In sum, the Information Assurance Program is endeavoring to solve a very large set of problems that grows larger every day.

We need good ideas and technology, cleverly integrated - sound, innovative systems engineering and integration is the cornerstone of the IA Program. We seek a systems solution rather than stovepipe fixes.

The program’s approach is to balance risk through complementary defense layers and tools. We are developing and improving security technologies in concert with the Information Technology Office and intend to integrate the evolving technologies with COTS.

The technologies will be integrated into the security architecture, which is an integral part of the AITS-RA. Security solutions will be tested in the AITS-RA architecture testbed with ongoing programs such as JFACC, BADD, and ALP. Realistic evaluation techniques such as Red Team exercises are planned to ensure system utility.

Information Assurance Program solutions will transition to the operational forces through the DII Leading Edge Services program.